UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
BALTIMORE DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	Case No.: 1:16-cr-469 JFM
	)	
MARTIN ROBERT HALL,	)	
	)	
Defendant.	)	

DEFENDANT'S MOTION TO SUPPRESS EVIDENCE
AND INCORPORATED MEMORANDUM IN SUPPORT

COMES NOW Defendant, Martin Hall, by and through counsel, aggrieved by unlawful searches and seizures made by the Baltimore County Police Department and the Department of Homeland Security, Immigrations and Custom Enforcement, and moves this Court to suppress any and all evidence and other items seized, test results concerning items seized, testimony or statements made about any of the foregoing, and any testimony regarding any observations made of Defendant's person while Defendant was under arrest or in custody that is intended to be used against Defendant.

The grounds for Defendant's motion are as follows:

1. That said articles which the Government intends to use against Defendant were obtained pursuant to unlawful searches and seizures by the Baltimore County Police Department and the Department of Homeland Security, Immigrations and Custom Enforcement.

2. The searches were not conducted pursuant to warrants supported by probable cause, and they were not justified by valid consent or other lawful justification.

3. The searches and seizures of data and electronic communications transmitted by Defendant's computer through the *Freenet* software constituted illegal searches under the Fourth Amendment and violated Defendant's Constitutional privacy rights.

4. The searches and seizures of Defendant's personal belongings, including but not limited to Defendant's computers, electronic devices, storage media and online accounts, constituted illegal searches under the Fourth Amendment and violated Defendant's Constitutional privacy rights.

5. All contents, including but not limited to all pictures and videos, that were found by way of the unlawful search and seizure of Defendant's laptop and hard drive were the poisonous fruit of said unlawful search and seizure as well as other violations of Defendant's Constitutional rights.

6. Said search and seizure thus violated Defendant's rights under the Fourth, Fifth, Sixth and Fourteenth Amendments to the United States Constitution.

MEMORANDUM IN SUPPORT OF MOTION TO SUPPRESS

I. Statement of Facts

Defendant is charged in this case with violations of 18 U.S.C. § 2252(a)(1) and (a)(5).

On September 1, 2016, Detective Josh Rees with the Baltimore County Police Department submitted a search warrant application for the search of Defendant's home. In his affidavit submitted with that application, Detective Rees stated the following with respect to the operation of the Freenet software (referred to in the affidavit as the "Network"):

> b) The Network is a distributed, Internet based, peer-to-peer network which attempts to let a user anonymously share files and chat on forums. The Network is free software and the source code is publicly available. Communications between computers running The Network, or nodes, are encrypted and routed through other Network nodes making it difficult to determine who is requesting the information and what the content is of the information being requested….
>
> c) Files, or parts of files, are stored in The Network using a key created from a compressed digital representation method called Secure Hash Algorithm Version 256 or SHA256.
>
> d) The Network breaks a file into small pieces, or blocks, each with a unique key based on this SHA256 value. These small blocks are then distributed across The Network users, or nodes, and stored in disk space provided by each user to The Network. No one user has the entire intact file. The keys to all of

> the parts of a file are found in a high level index block, or manifest computers running The Network software containing the key of a part of a file to retrieve from that node's data store, or to forward to another user that may have that part of the file.

Rees Affidavit at 5. His affidavit stated the following with respect to the purposes behind *Freenet* users' utilization of the software:

> h) The Network user connects to other users, unknown to them, or peers. They then send requests to these peers for the blocks of files they are attempting to download.
>
> i) The requests that a user of The Network sends to a peer contain only the key for the block of data and not the encryption password to make the data readable. A user relies on the inability of other users to decrypt a block of data or know what file contains this block to hide his use of The Network to obtain child pornography files.

Rees Affidavit at 6.

Detective Rees then went on to explain the operations of law enforcement using a modified version of the *Freenet* software:

> l) In April 2012, law enforcement officers began running copies of The Network software that had been modified for law enforcement to log the IP address, key, and date and time of requests that were sent to these law enforcement nodes. These keys are then compared to keys of known child pornography to identity IP addresses soliciting child pornography.
>
> m) Streams of requests for blocks of a particular file from an IP address can be evaluated to determine if the IP address is the likely requester of the file. This is done by analyzing data and certain characteristics of the request. This information is then calculated with an algorithm, which determines which users are actually making the original request for child pornography files. The goal of this law enforcement investigation is to target the original requester of child pornography files on The Network.

Rees Affidavit at 6. Detective Rees then went on to explain his own observations in reviewing data collected by law enforcement's operation of a modified version of the *Freenet* software, but without any context to allow a reviewing party to meaningfully evaluate the significance of his observations:

> 1) While reviewing requests received by undercover law enforcement nodes Your Affiant observed IP address 96.244.150.210 routing and/or requesting suspected child pornography file blocks. **The number and timing of the**

> **requests was significant enough to indicate that the IP address was the apparent original requester of the file.**
>
> 2) Your Affiant observed that on August 11, 2016 between 18:40:16 UTC and 02:32:10 UTC a computer running The Network software, at IP address 96.244.150.210, requested from The Network law enforcement nodes 87 parts, or blocks, of [a file described as constituting child pornography]…

Rees Affidavit at 6 (emphasis added). Detective Rees detailed seven other files, of which data suggested Defendant had requested 87, 79, 86, 81, 79, and 79 blocks respectively. Rees Affidavit at 8-9. The affidavit was silent as to the number of total blocks required to comprise a complete version of any of those files.

The affidavit of Det. Rees stated the following with respect to the purposes behind *Freenet* users' use of the software:

> The Network user connects to other users, unknown to them, or peers. They then send requests to these peers for the blocks of files they are attempting to download.
>
> i) The requests that a user of The Network sends to a peer contain only the key for the block of data and not the encryption password to make the data readable. A user relies on the inability of other users to decrypt a block of data or know what file contains this block to hide his use of The Network to obtain child pornography files.

Rees Affidavit at 6.

Detective Rees's warrant application was granted, and the search warrant was issued, on September 1, 2016. On September 7, 2016, officers with the Baltimore County Police Department executed a search and seizure warrant at Defendant's home, and seized a number of computers, electronic devices, and storage media.

On September 12, 2016, Special Agent Christine Carlson ("S.A. Carlson") presented an application and affidavit for a search warrant to search the electronic items seized from Defendant's residence for evidence of child pornography and contents of Defendant's Google account. Her affidavit was based primarily on the alleged discovery of a number of child pornography images during the examination of computers on scene at the time of the

execution of the September 1, 2016 search warrant by use of the forensic tool OS Triage. Detective Rees's warrant application was granted, and the search warrant was issued, on September 12, 2016. Pursuant to the execution of that warrant, law enforcement seized a number of other suspected child pornography files.

II. Defendant had a Legitimate Expectation of Privacy in Transmissions Routed from His Computer Using *Freenet,* and the Interception and Logging of the Data and Content of These Transmissions Constituted an Unlawful Search and Seizure

The Fourth Amendment provides that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV . "The Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz v. United States*, 389 U.S. 347, 351 (1967). "But **what he seeks to preserve as private**, even in an area accessible to the public, may be constitutionally protected." *Id*. (emphasis added). *See also United States v. Jones*, 565 U.S. 400, 403 (2012) (excluding GPS evidence recording publicly observable information about vehicle location on Fourth Amendment grounds).

"[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001), citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). In determining whether an individual has a legitimate expectation of privacy, courts consider: (1) whether the individual, by his conduct has subjectively exhibited an actual subjective expectation of privacy; and (2) whether that subjective expectation is "one that society is prepared to recognize as 'reasonable.'"*Kyllo*, 533 U.S. at 33 ("As Justice Harlan's oft-quoted concurrence described it, a Fourth Amendment search occurs when the government violates a

subjective expectation of privacy that society recognizes as reasonable."). *See also Katz*, 389 U.S. at 351-53.

The use of technology to conduct a search implicates different considerations than an investigation relying only on ordinary human observation. "Where . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant." *Kyllo*, 533 U.S. at 40. In *Kyllo*, the Court held that the use of thermal imaging to obtain information from the interior of a home "that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,'…constitutes a search -- at least where…the technology in question is not in general public use." *Id.* (internal citations and quotations omitted). *See also Florida v. Jardines*, 133 S. Ct. 1409, 1411-12 (2013) (holding that an unlicensed physical intrusion upon property by using a drug sniffing dog at the front door of a home constitutes a search under the Fourth Amendment).

In *Jones*, the Government "installed a GPS tracking device on the undercarriage of the [defendant's] Jeep while it was parked in a public parking lot." *Jones*, 565 U.S. at 403. "Over the next 28 days, the Government used the device to track the vehicle's movements, and once had to replace the device's battery when the vehicle was parked in a different public lot in Maryland." *Id.* "By means of signals from multiple satellites, the device established the vehicle's location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer." *Id.* "It relayed more than 2,000 pages of data over the 4-week period." *Id.*

While the holding of four Justices in *Jones* rested on a trespassory theory of the Fourth Amendment, the Supreme Court has repeatedly affirmed that the Fourth Amendment is not only concerned with trespassory intrusions on physical property, as the *Jones* Court

itself recognized. "In *Katz*, [the] Court enlarged its then-prevailing focus on property rights by announcing that the reach of the Fourth Amendment does not 'turn upon the presence or absence of a physical intrusion.'" *Jones*, 565 U.S. at 414), citing *Katz*, 389 U.S. at 353. Instead, *Katz* distinguished between what an individual has "knowingly expose[d] to the public" and "what he seeks to preserve as private, even in an area accessible to the public," when determining whether the Fourth Amendment's protections apply. *Katz*, 389 U.S. at 353. *See id.* (attaching an electronic listening device to the outside of a public phone booth without a warrant was an unreasonable search under the Fourth Amendment because the user "justifiably relied" on the privacy of the phone booth); *Jones*, 565 U.S. at 404 (the government's installation of a GPS device on a vehicle parked in a public parking lot, and the use of that device to track the vehicle's subsequent movements, constituted a search under the Fourth Amendment and thus required a warrant).

In Justice Sotomayor's *Jones* concurrence, she noted that she would "take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements." *Id.* at 416 (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on"). Justice Sotomayor also wrote that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Id.* at 417. "This approach," she wrote, "is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Id.* "People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online

retailers." *Id.* Similarly, in *Jardines*, Justice Kagan observed that deciding what constitutes a "search" under the Fourth Amendment could be performed by looking at privacy interests rather than property rights. *Jardines*, 133 S. Ct. at 1418-19 (Kagan, J., concurring). Describing what her opinion would have looked like under a privacy interests analysis, she wrote that her opinion "would have determined that police officers invade those shared expectations when they use trained canine assistants to reveal within the confines of a home what they could not otherwise have found there." *Id.*

Although "[t]he Supreme Court has held that addressing and other routing information on paper letters, like pen-register and trap-and-trace information (including the date and time of listed calls) regarding telephone calls, is accessible to the government without a warrant," courts have recognized that the communication's **contents** are still protected. *United States v. Davis*, 785 F.3d 498, 529 n.5 (11th Cir. 2015) (Rosenbaum, J., concurring), citing *Ex parte Jackson*, 96 U.S. 727, 736 (1877), *Smith*, 442 U.S. at 735; *see also United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) ("we hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP.") (internal quotation omitted); *Smith*, 442 U.S. at 741-43 (the warrantless use of a "pen register" at the telephone company to determine the telephone numbers dialed from a particular home was permissible under the Fourth Amendment because defendant did not have a "legitimate expectation of privacy" in the numbers dialed, where the *contents* of the communication were not determinable from the pen register).

In the instant case, law enforcement's interception and logging of data and content transmitted through the use of modified copies of *Freenet* constituted an unlawful search. Law enforcement was not merely penning or trapping and tracing Defendant's IP address or other data through its use of the modified *Freenet*. Officers were also intercepting and

logging the **content** of the electronic communications routed from Defendant's computer, not merely identifying information. Such content is analogous to other electronic communications, such as email content, except that substantially more secure protections of content and anonymity are intentionally applied in the case of *Freenet* communications than email communications through an internet service provider—in fact, such protections are the fundamental purpose of the Freenet software and its use. Defendant had a reasonable expectation of privacy in electronic communications both originating and forwarded from his computer using *Freenet*, and law enforcement intercepted, logged, and tracked these communications and content without a search warrant using technology not in general, public use.

Defendant had the requisite actual and subjective belief that the communications and content sent from and routed through his computer would be private, and he intentionally used the *Freenet* service to maintain that anonymity and privacy, and in so doing, he manifested that subjective belief. Defendant's subjective expectation of privacy in *Freenet* communications and content is, moreover,one that society recognizes as reasonable.

Internet users often seek anonymity and privacy for free speech purposes, and the existence and popularity of the *Freenet* service and others like it is evidence that this expectation of privacy is one that society both values and recognizes as reasonable. Moreover, the electronic communications and content sent through *Freenet* are functionally indistinguishable from that sent in an email. Courts have recognized that email users have a legitimate expectation of privacy in the content of their emails, just as they have in the content of communications sent by postal mail, and Congress has made interception of those messages a felony criminal offense. *Warshak*, 631 F.3d at 288; *Forrester*, 512 F.3d at 511; *United States v. Councilman*, 418 F.3d 67, 79 (1st Cir. 2005) (holding that the interception of e-mail messages that had already been sent and were in "transient electronic storage," such as

on a hard drive or in RAM, constitutes an "interception" under Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, and a criminal offense). There is no logical basis for distinguishing the contents of email communications from the contents of *Freenet* communications, which are also "electronic communications" under ECPA/Wiretap Act standards. In fact, *Freenet* users have expressed and sought an even heightened expectation of privacy because of the affirmative steps they take to ensure the anonymity and privacy of their communications, which are more stringent than those taken by typical email users.

Freenet is software that intentionally obscures the communications transmitted by users by encrypting the information and decentralizing the system of delivery, ensuring that the content of the communications is not identified or observed by other users by use of an entirely automated electronic process. Appellant and other users of *Freenet* have thus taken decisive, intentional steps to protect the privacy of their communications, and have gone to greater lengths to protect their privacy than do typical users of other electronic communication mediums, such as e-mail and text messages. Courts have recognized a legitimate, protected privacy interest in the content of communications such as e-mail and text messages, and even in non-electronic communications such as postal mail and landline telephone conversations, where users have taken only the minimum steps required to maintain their privacy. *See Katz*, 389 U.S. at 352 (closing the door of a public telephone booth is sufficient to protect the privacy interest in the communication); *United States v. Van Leeuwen*, 397 U.S. 249, 251 (1970), citing *Ex parte Jackson*, 96 U.S. at 733 (a sealed letter or package sent through the postal mail is protected from search by the Fourth Amendment); *Warshak*, 490 F.3d at 470 (finding a protected privacy interest in emails generally, and noting that simply because an email is routed through third parties or intermediaries does not affect the privacy of the communication, just as routing a non-electronic communication through

the phone company or the post office does not alter the privacy of those communications).

To hold in this case that Appellant's intentional use of *Freenet* did not sufficiently protect his privacy interest in the content and communications, despite the great lengths taken to preserve that privacy in comparison with the minimal privacy protections of other forms of communication already recognized as protected, would fly in the face of *Katz*. A communication sent through *Freenet*, a software specifically engineered to maintain an extremely protective level of anonymity and privacy, must at least be granted the same Fourth Amendment protection as a telephone conversation in a public telephone booth, a letter, or an email sent through a basic Gmail or Hotmail account. If a *Freenet* communication is not recognized as private in transit, it is difficult to imagine that *any* form of electronic communication could enjoy Fourth Amendment protection. The courts, through decisions like *Katz* and *Warshak*, and Congress, through ECPA, have strongly suggested there is a legitimate right to privacy in electronic communications in appropriate circumstances. *Freenet* communications represent heavily encrypted and protected electronic communications intentionally aimed at "closing the door" on outside interference and monitoring. They must be deemed protected under the Fourth Amendment if *any* electronic communication is to be protected. Defendant had a legitimate expectation of privacy in the content of *Freenet* communications, and law enforcement's warrantless search of his private *Freenet* transmissions constitutes an unreasonable search under the Fourth Amendment.

III. Law Enforcement's Use of Modified *Freenet* Software and Nodes to Log IP Address, Key, and Date and Time of Requests, Without Prior Judicial Authorization, Constituted an Unlawful Search Under the Electronic Communications and Protection Act That Violated Reasonable Expectations of Privacy Recognized Under that Act

Enacted in 1986, the Electronic Communications Privacy Act ("ECPA") updated the Federal Wiretap Act of 1968 ("Wiretap Act") to make it apply to other types of electronic communications. ECPA in its entirety "protects wire, oral, and electronic communications

while those communications are being made, are in transit, and when they are stored on computers." U.S. Department of Justice, *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22*, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285. "The Act applies to email, telephone conversations, and data stored electronically." *Id.*

Both ECPA and the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2712, require that law enforcement go through appropriate application and affidavit procedures before a judge can enter an ex parte order authorizing or approving interception of wire, oral, **or electronic communications** or retrieval of stored electonic communications. *See* 18 U.S.C. § 2518(1)-(3) (emphasis added). Under ECPA, an "application for an order authorizing or approving the interception of a wire, oral, or electronic communication…shall be made in writing upon oath or affirmation to a judge of competent jurisdiction and shall state the applicant's authority to make such application." 18 U.S.C. § 2518(1) (emphasis added). The same section sets forth the information required to be contained in each application under ECPA. *Id.* Such an application allows the judge to determine whether there exists probable cause for an interception to take place. *See* 18 U.S.C. § 2518(3). No such order was sought in this case before law enforcement intercepted and stored communications between the Freenet node associated with Defendant and the node utilized by law enforcement.

Under ECPA, the term "'intercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device;" and "'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8). An "electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic

or photooptical system that affects interstate or foreign commerce," outside of some specified exceptions that do not apply in this case. 18 U.S.C. § 2510(12).

ECPA itself provides remedies for persons aggrieved by violations of the Act, and criminalizes violations of the Act, including violations related to electronic communications. *Id.* Although ECPA does not provide an independent exclusionary rule for "electronic communications," as it does for wire and oral communications, the fact that Congress enacted ECPA and specifically provided protections, including criminal penalties, for "electronic communications" of the sort at issue here provides compelling evidence that Congress has recognized the legitimacy of a privacy interest in electronic communications like Defendant's computer's activity on *Freenet*. 18 U.S.C. §§ 2511, 2515; *Councilman*, 418 F.3d at 79 (holding that the interception of e-mail messages that had already been sent and were in "transient electronic storage," such as on a hard drive or in RAM, constitutes a criminal "interception" under the Wiretap Act). *See also* Ryan A. Ray, *The Warrantless Interception of E-Mail: Fourth Amendment Search or Free Rein for the Police?*, 36 RUTGERS COMPUTER & TECH. L.J. 178, 219 (2010).

In this case, law enforcement officers in Baltimore County or elsewhere began running copies of *Freenet* that had been modified for law enforcement to log the IP address, key, and date and time of requests that were sent to these law enforcement *Freenet* nodes. This data unquestionably constitutes "electronic communications" under 18 U.S.C. § 2510. Law enforcement officers intercepted the data by logging it through use of the modified *Freenet*. These officers acquired the **content** of the transmissions at issue and used that content to match files' identifying data ("hash value") to known files, and stored the data they had intercepted.

In doing so, Defendant anticipates that witnesses will testify that the underlying law enforcement officers never applied for authorization to intercept such information, pursuant

to 18 U.S.C. § 2518(1),[1] and at no time did law enforcement possess a warrant for such a search. Defendant anticipates that law enforcement did not return any of the requested files and therefore was never itself a party to the communications, but instead served as a conduit for the communications in an analogous role to that of an internet service provider. 18 U.S.C. § 2511(2)(a) and (c) ("It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a **party** to the communication or one of the parties to the communication has given prior consent to such interception") (emphasis added). In so doing, law enforcement acted outside any authorization provided by the Act "for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication" to render its service. 18 U.S.C. § 2511(2)(a). *See also Campbell v. Facebook Inc*., 77 F.Supp.3d 836 (N.D. Cal. 2014) ("any consent with respect to the processing and sending of messages itself does not necessarily constitute consent to the specific practice alleged in this case—that is, the scanning of message content for use in targeted advertising"); *see also Councilman*, 418 F.3d at 79 (holding that the interception of e-mail messages that had already been sent and were in "transient electronic storage," such as on a hard drive or in RAM, constitutes a criminal "interception" under the Wiretap Act). The electronic communications made through *Freenet* were thus intercepted by law enforcement in violation of ECPA.

While ECPA itself contains no exclusionary provision for such illegally intercepted information, suppression of the information obtained through law enforcement's interception of data using the modified *Freenet* service is nevertheless proper. Congress recognized Defendant's legitimate expectation of privacy in such communications by enacting ECPA

[1] Law enforcement likewise appears to have failed to request authorization to access the electronic communications stored by its modified Freenet node, in violation of the Stored Communications Act, 18 U.S.C. §§ 2701-2712.

and specifically protecting the privacy of those communications and penalizing violations as felony offenses under 18 U.S.C. § 2511. Defendant likewise intentionally availed himself of additional protection by using *Freenet* to make his electronic communications even more private and anonymous. The general exclusionary rule under the Fourth Amendment applies to require that the evidence obtained by law enforcement in violation of Defendant's subjective expectations of privacy, an expectation that has been recognized as reasonable by society and that is reflected in ECPA, was violated by law enforcement's interception, storage, search and seizure of Defendant's electronic communications and/or those of his computer and all evidence seized in this case should be suppressed.

IV. Defendant Expects to Establish that the Judge Issuing the September 7, 2016 Search Warrant Lacked the Technological Expertise to Determine Probable Cause Based on the Contents of the Affidavit, and Improperly Based His Determination on Conclusory Statements in the Affidavit, Thus Serving as a Rubber Stamp for Law Enforcement

The Supreme Court has held that, in issuing a search warrant, "an issuing magistrate must meet two tests." *Shadwick v. City of Tampa*, 407 U.S. 345, 350 (1972). "He must be neutral and detached, and he must be capable of determining whether probable cause exists for the requested arrest or search." *Id.* "The primary reason for the warrant requirement is to interpose a 'neutral and detached magistrate' between the citizen and 'the officer engaged in the often competitive enterprise of ferreting out crime.'" *United States v. Karo*, 468 U.S. 705, 717 (1984), quoting *Johnson v. United States*, 333 U.S. 10, 14 (1948).

Although reviewing courts give "great deference" to a magistrate's determination of probable cause, "[d]eference to the magistrate . . . is not boundless." *United States v. Leon*, 468 U.S. 897, 914 (1984). A reviewing court must first inquire "into the knowing or reckless falsity of the affidavit on which that determination was based." *Id.*, citing *Franks*, 438 U.S. 154. "Second, the courts must also insist that the magistrate purport to 'perform his neutral and detached function and not serve merely as a rubber stamp for the police.'" *Id.*, quoting

Aguilar v. Texas, 378 U.S. 108, 111 (1964); *see also Illinois v. Gates*, 462 U.S. 213, 239 (1983). "Third, reviewing courts will not defer to a warrant based on an affidavit that does not 'provide the magistrate with a substantial basis for determining the existence of probable cause.'" *Leon*, 468 U.S. at 915, quoting *Gates*, 462 U.S. at 239.

Under the substantial basis prong of the *Leon* analysis, "[s]ufficient information must be presented to the magistrate to allow that official to determine probable cause; his action cannot be **a mere ratification of the bare conclusions of others**." *Gates*, 462 U.S. at 239 (emphasis added); *see also United States v. Farlee*, 910 F. Supp. 2d 1174, 1184 (D.S.D. Dec. 7, 2012) ("The *Gates* Supreme Court decision guides the determination of when an affidavit is too conclusory to support issuance of a warrant."). Wholly conclusory statements in a warrant application ordinarily will not suffice. *See Gates*, 462 U.S. at 239 (citing *Nathanson v. United States*, 290 U.S. 41 (1933) and *Aguilar v. Texas*, 378 U.S. 108 (1964)). The good-faith exception to the exclusionary rule does not apply to a "bare bones" affidavit, because a magistrate "could not have acted as other than a 'rubber stamp' in approving such an affidavit." *United States v. DeQuasie*, 373 F.3d 509, 521 (4th Cir. 2004). A "bare bones" affidavit is "one that contains 'wholly conclusory statements, which lack the facts and circumstances from which a magistrate can independently determine probable cause.'" *United States v. Wilhelm*, 80 F.3d 116, 121 (4th Cir.1996) (quoting *United States v. Laury*, 985 F.2d 1293, 1311 n. 23 (5th Cir.1993)). Accord *United States v. Williams*, 224 F.3d 530, 533 (6th Cir.2000) ("a 'bare bones' affidavit is similar to, if not the same as, a conclusory affidavit. It is one which states only the affiant's belief that probable cause existed")

On review, the court's duty "'is simply to ensure that the magistrate had a substantial basis for concluding that probable cause existed.'" *United States v. Hodge*, 354 F.3d 305, 309 (4th Cir. 2009) (quoting *Gates*, 462 U.S. at 238-39); *see United States v. Bynum*, 293 F.3d 192, 202 (4th Cir. 2002). Nevertheless, there are "limits beyond which a magistrate may not

venture in issuing a warrant," *Gates*, 462 U.S. at 239, 103 S.Ct. 2317, and "[d]eference to the magistrate ... is not boundless." *United States v. Leon*, 468 U.S. 897, 914 (1984). "Sufficient information must be presented to the magistrate to allow that official to determine probable cause; his actions cannot be a mere ratification of the bare conclusions of others." *Gates*, 462 U.S. at 239. Therefore, "the Government cannot rely upon post hoc rationalizations to validate those seizures that happen to turn up contraband." *United States v. Foster*, 634 F.3d 243, 249 (4th Cir. 2011).

The reason that conclusory statements in a law enforcement affidavit cannot be the basis of probable cause for issuance of a search warrant is that the judge, not law enforcement, is the proper party to draw inferences and conclusions from the facts. "The essential protection of the warrant requirement of the Fourth Amendment . . . is in 'requiring that [the usual inferences which reasonable men draw from evidence] be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.'" *Gates*, 462 U.S. at 240, quoting *Johnson v. United States*, 333 U.S. 10, 13-14 (1948).

Here, the *Leon* analysis applies, first, because Detective Rees failed to provide sufficient information to enable the reviewing magistrate to make an independent assessment of probable cause. This problem was compounded by the technical and complicated nature of the matters alleged in the affidavit, and by the improperly conclusory nature of the statements connected with *Freenet* provided in the affidavit. Defendant expects to introduce evidence at hearing that will establish the magistrate's unfamiliarity with *Freenet* and relevant concepts of computer science. Under these circumstances, the issuing magistrate court could not have functioned in its intended role. As a result, Defendant's constitutional rights were violated by the issuance of the September 1, 2016 search warrant, and the evidence searched and seized during the execution of that warrant should be suppressed. Because the September 12, 2016

search warrant was based overwhelmingly on evidence seized pursuant to the earlier search warrant, all evidence seized pursuant to the September 12, 2016 search warrant should likewise be suppressed.

V. Conclusion

WHEREFORE, Defendant Martin Hall respectfully requests that this Court issue an order excluding all of the above-referenced evidence from trial, and for such further relief as this Court deems just and proper.

Respectfully submitted,

ROSENBLUM, SCHWARTZ, ROGERS & GLASS, PC

By: /S/ Adam D. Fein
ADAM D. FEIN, #52255 MO
Attorney for Defendant
120 S. Central Avenue, Suite 130
Clayton, Missouri 63105
(314) 862-4332
Facsimile (314)862-8050
Email: afein@rsrglaw.com

CERTIFICATE OF SERVICE

I hereby certify that on May 9, 2016, the foregoing was electronically filed with the Clerk of the Court to be served by operation of the Court's electronic filing system upon Mr. Paul E. Budlow and Ms. Kaylynn Shoop, assistant United States attorneys.